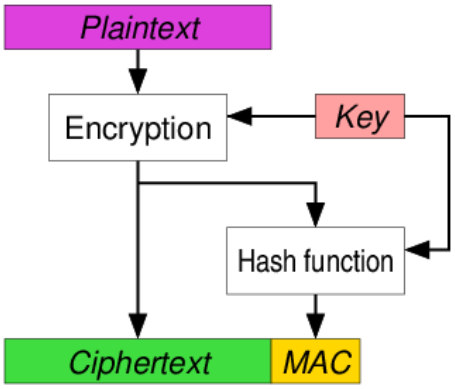
Pergunta 3

Para a resolução deste problema temos de encontrar uma maneira de proteger a informação sensível e para isso dispomos de 3 soluções: *Encrypt then Mac, Encrypt and Mac, Mac then Encrypt*. A alternativa escolhida é a primeira.

Encrypt-then-MAC

Neste caso começamos por utilizar a chave secreta para cifrar a nossa informação e de seguida utilizamos o HMAC e uma outra chave secreta para criar uma hash do criptograma.



A única diferença do esquema apresentado e do esquema a utilizar neste caso é que em vez de calcularmos o hash de apenas o criptograma, calculamos o hash do criptograma+etiqueta. Assim este método fornece a integridade do criptograma e da etiqueta assim como do plaintext. Além disso o MAC não contem nenhuma informação sobre o plaintext diretamente e apesar de conter informação sobre a etiqueta, esta não contem nenhuma informação sensível (protegendo-nos de eventuais falhas que possam ser descobertas no mecanismo utilizado para o calculo do MAC).

Algoritmo pseudocódigo

```
#Processo de cifrar
criptograma = cifra(plaintext)
criptograma = criptograma+etiqueta+size_Etiqueta
mac = hmac(k,criptograma)
res=criptograma+ mac

#Processo de decifrar
mac = extraiMac(res)
criptograma = extraiCriptograma(res)
mac_calculado= hmac(k,criptograma)
if mac != mac_calculado: erro (“macs não coincidem”)
etiqueta = extraiEtiqueta(criptograma)
segredo = decifrar(criptograma)
```